Cybersecurity Incident Response And Potential Economic Impact Of A Cyber Crisis

PISA, 16 FEB 2023

MATTEO REDAELLI

~ $ whoami
Matteo Redaelli

Current Roles

10+ Years of Experience in Incident Response

- **Incident Response ICEG Lead** – Accenture Security
  - Security Sr. Manager
- **Adjunct Professor of Security Risk Management** – Università Insubria

Education

- BSc & MSc in Computer Science
  - Università degli Studi di Milano Bicocca – Italy
  - UIT Tromsø – Norway

EMBA Candidate 2024

- SDA Bocconi Milano

@solventred

https://www.linkedin.com/in/redaelli/

GCFA GCIH GRID CISM

Introduction to Incident Response

Event
INTRODUCTION

An “event" **is an observable and measurable occurrence in a system and/or network.**

Examples of events include:

- The system boot sequence
- The system crash
- A firewall that prevents a connection attempt

Computer Security Incident
INTRODUCTION

A computer security incident is any action or activity – accidental or deliberate – **that compromises the confidentiality, integrity, or availability of data and information technology resources.**

Incidents also include the use of technology for criminal activities such as: fraud, piracy, theft, copyright infringement, unauthorized penetration testing etc…

An incident is an event that implies harm, or the attempt to harm.

LEVEL 1 Low Severity
INCIDENT LEVEL CLASSIFICATION

FOR REFERENCE

A level 1 incident is any incident that has a low impact to the organization information technology resources and is contained within the company unit.

The following criteria define **level 1** incidents:

1. Data classification: Unauthorized disclosure of confidential information has not occurred.
2. Legal issues: Lost or stolen hardware that has low monetary value or is not part of a mission critical system.
3. Business impact: Incident does not involve mission critical services.
4. Expanse of service disruption: Incident is within a single unit.
5. Threat potential: Threat to other information technology resources is minimal.
6. Public interest: Low potential for public interest.
7. Policy infraction: Security policy violations determined by the organization.

LEVEL 2 Moderate Severity
INCIDENT LEVEL CLASSIFICATION

FOR REFERENCE

A level 2 incident is any incident that has a moderate impact to organization information technology resources and is contained within the unit.

The following criteria define **level 2** incidents:

1. Data classification: Unauthorized disclosure of confidential information has not been determined.
2. Legal issues: Lost or stolen hardware with high monetary value or that is part of mission critical system.
3. Business impact: Incident involves mission critical services.
4. Expanse of service disruption: Incident affects multiple units within the organization.
5. Threat potential: Threat to other company information technology resources is possible.
6. Public interest: There is the potential for public interest.
7. Policy infraction: Security policy violations determined by the organization.

LEVEL 3 High Severity
INCIDENT LEVEL CLASSIFICATION

FOR REFERENCE

A level 3 incident is any incident that has impacted or has the potential to impact other external information technology resources and/or events of public interest.

The following criteria define **level 3** incidents:

1. Data classification: Unauthorized disclosure of confidential information has occurred outside the organization.
2. Legal issues: Incident investigation and response is transferred to law enforcement.
3. Business impact: Threat to other organization information technology resources is high.
4. Expanse of service disruption: Disruption is wide spread across the organization and/or other entities.
5. Threat potential: Incident has potential to become wide spread across the organization and/or threatens external, third-party information technology resources.
6. Public interest: There is active public interest in the incident.
7. Policy infraction: Security policy violations determined by the organization.

Incident Response
INTRODUCTION

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident.

The goal is **to handle the situation in a way that limits damage** (by preserving the confidentiality, integrity and availability of enterprise information assets) and reduces recovery time and costs.

Incident Handling is defined as the summary of processes and predefined procedural actions to effectively and actionably handle/manage an incident.

Incident Response Goals

INTRODUCTION

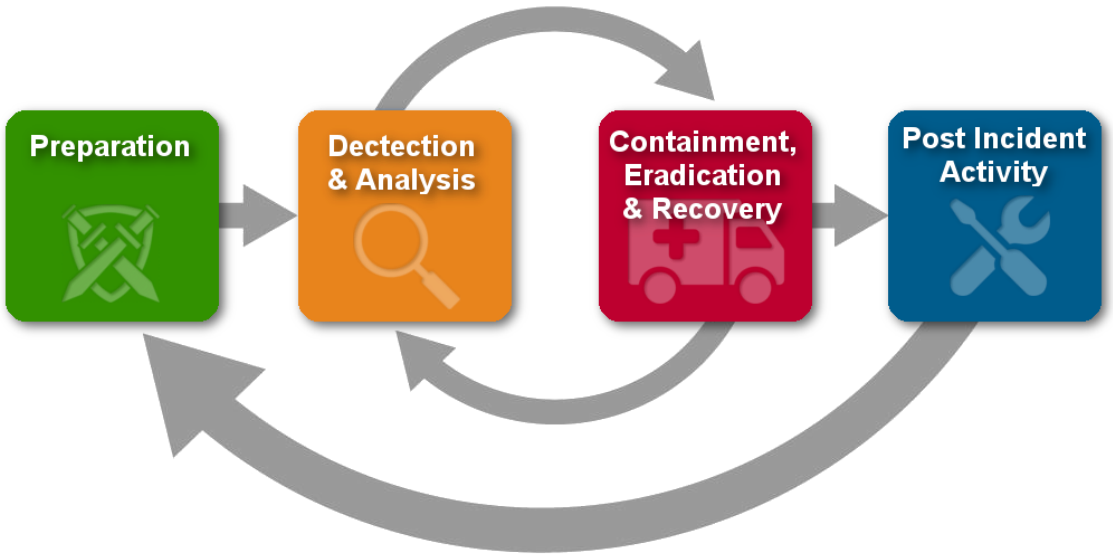
- Preserving the confidentiality, integrity and availability of enterprise information assets.
- Minimizing the impact of the incident.
- Providing management with sufficient information to decide on appropriate course of action.
- Providing a structured, logical, repeatable, and successful approach.

Incident Response Plan
INTRODUCTION

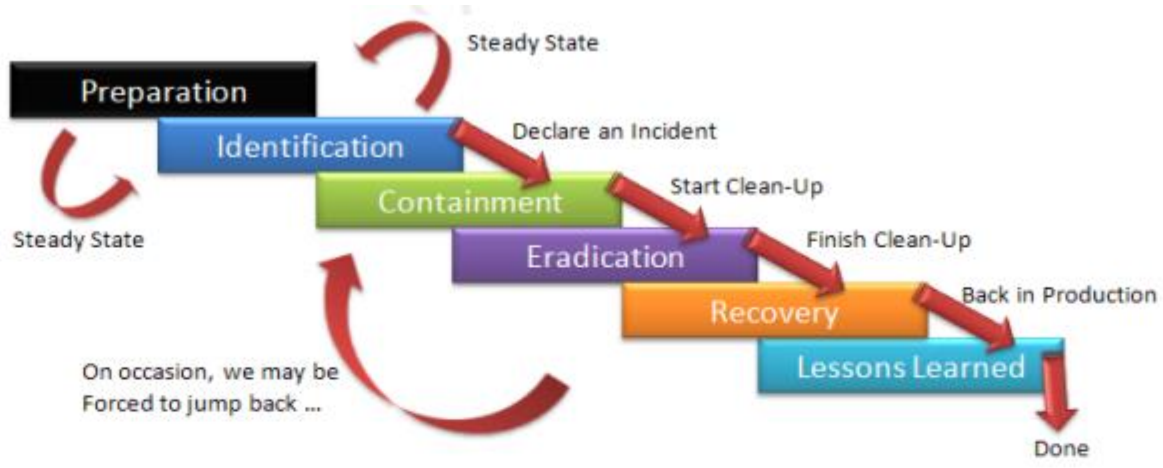
- Incident response (IR) is an organization’s set of planning and preparation efforts for detecting, reacting to, and recovering from an incident
- Incident response planning (IRP) consists of the actions taken by senior management to develop and implement the IR policy, plan, and computer security incident response team
- The IR Plan is the documented product of incident response planning; a plan that shows the organization’s intended efforts in the event of an incident

Incident Response Steps
INTRODUCTION

NIST - 4 STEPS



SANS - 6 STEPS



Preparation Phase - Introduction

INCIDENT RESPONSE

This phase will be the pillar of an incident response planning.

Part of this phase includes:

- Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of data breach.
- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Response plan should be well documented, thoroughly explaining everyone’s roles and responsibilities. Then the plan must be tested in order to assure that your employees will perform as they were trained. The more prepared your employees are, the less likely they’ll make critical mistakes.

Preparation Phase
INCIDENT RESPONSE

Questions to address

- Has everyone been trained on security policies?
- Have your security policies and incident response plan been approved by appropriate management?
- Does the Incident Response Team know their roles and the required notifications to make?

Preparation Phase
INCIDENT RESPONSE

Critical elements that should be prepared in advance:

- **Policy**—define principle, rules and practices to guide security processes. Ensure the policy is highly visible both to employees and users, for example by displaying a login banner that states all activities will be monitored, and clearly stating unauthorized activities and the associated penalties.
- **Response Plan/Strategy**—create a plan for incident handling, with prioritization of incidents based on organizational impact. For example, organizational impact is higher the more employees are affected within the organization, the more an event is likely to impact revenues, or the more sensitive data is involved, such as salaries, financial or private customer data.
- **Communication—**create a communication plan that states which CSIRT (Computer Security Incident Response Team) members should be contacted during an incident, for what reasons and when they can be contacted. For example, there may be operations staff on call at all hours, everyone in the organization should know, which incident responders to contact to help bring systems back up. The communication plan should state the policy for contacting law enforcement, and who should make contact.
- **Documentation**—documentation is not optional and can be a life saver. If the incident is considered a criminal act, your documentation will be used to press charges against suspects. Any information you collect about the incident can also be used for lessons learned and to improve your incident response process. Documentation should answer the questions: Who, What, When, Where, Why, and How?.

Preparation Phase
INCIDENT RESPONSE

Team—**build a CSIRT team with all relevant skills, not just security.** Include individuals with expertise in security but also IT operations, legal, human resources, and public relations—all of whom can be instrumental in dealing with and mitigating an attack.

Access control—**make sure that CSIRT staff have the appropriate permissions to do their job.** It is a good idea to have, as part of the incident response plan, network administrators add permissions to CSIRT member accounts, and then remove them when the incident is over.

Training—**ensure initial and ongoing training for all CSIRT members on incident response processes, technical skills and relevant cyberattack patterns and techniques.** Carry out drills at regular intervals to insure that everyone in the CSIRT knows what they need to do and is able to perform their duties during a real incident.

- https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/ ➔ Nice card game for creating incident scenarios.

Tools—**evaluate, select and deploy software and hardware that can help respond to an incident more effectively**. All of the tools should be packaged in a "jump bag" that can be quickly accessed by CSIRT members when an incident occurs.

Preparation Phase Team Definition

INCIDENT RESPONSE

- Identify qualified people to join the team a multi-disciplinary team is the best choice:
  - Security (Computer Security and Physical Security)
    - (Incident Handler, Forensic Analyst, Malware Analyst)
  - Operations (System Administration)
  - Network Management
  - Legal Consultant
  - HR
  - Public affairs and relations
  - Disaster Recovery and/or Business Continuity Planning

Preparation Phase Team - Getting Access to data and systems
INCIDENT RESPONSE

The **incident response team needs to be able to access systems**

- Passwords for critical systems and cryptographic keys. Or work with people who have access (pwd, keys..) to the systems.

Work with the operation team, notifying them before logging into the machines

Use incident handlers **with the skills needed to admin the specific operating systems**

Preparation Phase Team – Jump Bag

INCIDENT RESPONSE

Get a duffle bag and keep it stocked with items for incident handling:

Software (e.g. Forensic software, binary image creation software, bootable OS)

Hardware (e.g. USB, HDD external, ethernet tap, patch cables, laptop with different operating systems, a lot of RAM, lots of hard disk space)

Other (e.g. List of emergency numbers, telephone with extra battery, notebooks, screwdrivers, pens)

Proper Clothing: (Data Centers are cold)

Preparation Phase Team – Jump Bag

INCIDENT RESPONSE

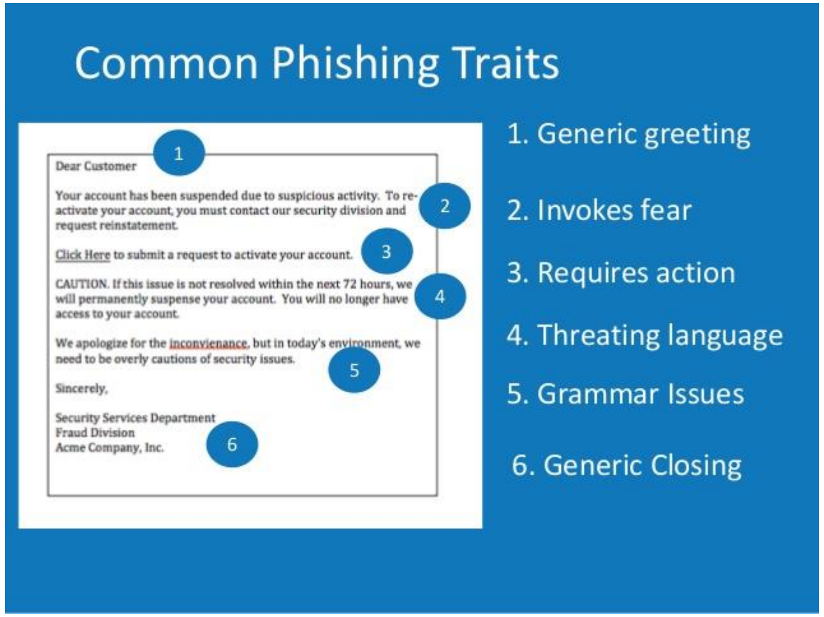
Velociraptor is an advanced digital forensic and incident response tool that enhances your visibility into your endpoints.

- At the press of a (few) buttons, perform targeted collection of digital forensic evidence simultaneously across your endpoints, with speed and precision.
- Continuously collect endpoint events such as event logs, file modifications and process execution. Centrally store events indefinitely for historical review and analysis.
- Don't wait until an event occurs. Actively search for suspicious activities using our library of forensic artifacts, then customize to your specific threat hunting needs.

https://docs.velociraptor.app/

Preparation Phase – People

INCIDENT RESPONSE



Common Phishing Traits

Dear Customer

Your account has been suspended due to suspicious activity. To re-activate your account, you must contact our security division and request reinstatement.

Click Here to submit a request to activate your account.

CAUTION. If this issue is not resolved within the next 72 hours, we will permanently suspense your account. You will no longer have access to your account.

We apologize for the inconvienance, but in today's environment, we need to be overly cautions of security issues.

Sincerely,

Security Services Department
Fraud Division
Acme Company, Inc.

1. Generic greeting
2. Invokes fear
3. Requires action
4. Threating language
5. Grammar Issues
6. Generic Closing

One of the most overlooked aspects of our security posture also, the most easily attacked

- Spear Phishing
- Social Engineering

Reoccurring training can be a great help

Annual training tends to be ineffective; they must be constant.

You can test your users with social engineering calls or phishing tests

https://docs.velociraptor.app/

Identification Phase
INCIDENT RESPONSE

This is the process where you determine whether you've been breached. A breach, or incident, could originate from many different areas.

- **Monitor**: Monitor security events in your environment using firewalls, intrusion prevention systems, and data loss prevention.
- **Detect**: Detect potential security incidents by correlating alerts within a SIEM solution.
- **Alert**: Analysts create an incident ticket, document initial findings, and assign an initial incident classification.
- **Report:** Your reporting process should include accommodation for regulatory reporting escalations

Questions to address:

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?

Has the source (point of entry) of the event been discovered?

Identification Phase
INCIDENT RESPONSE

Setting up monitoring for all sensitive IT systems and infrastructure.

Analyzing events **from multiple sources including log files, error messages, and alerts** from security tools.

Identifying an incident by **correlating data from multiple sources**, and reporting it as soon as possible.

Notifying CSIRT members and **establishing communication with a designated command center** (for example this could be senior management, IT operations)

Documenting everything that incident responders are doing as part of the attack—answering the Who, What, Where, Why, and How questions.

Threat prevention and detection capabilities across all main attack vectors.

Identification Phase – Assign an Incident Manager

INCIDENT RESPONSE

- Once an incident has been declared, a person should be assigned as the primary incident handler.
- Keep at least one person to handle identification and assessment
- Assign a specific set of events on a specific set of system to analyze.
- Empower him to escalate if needed.

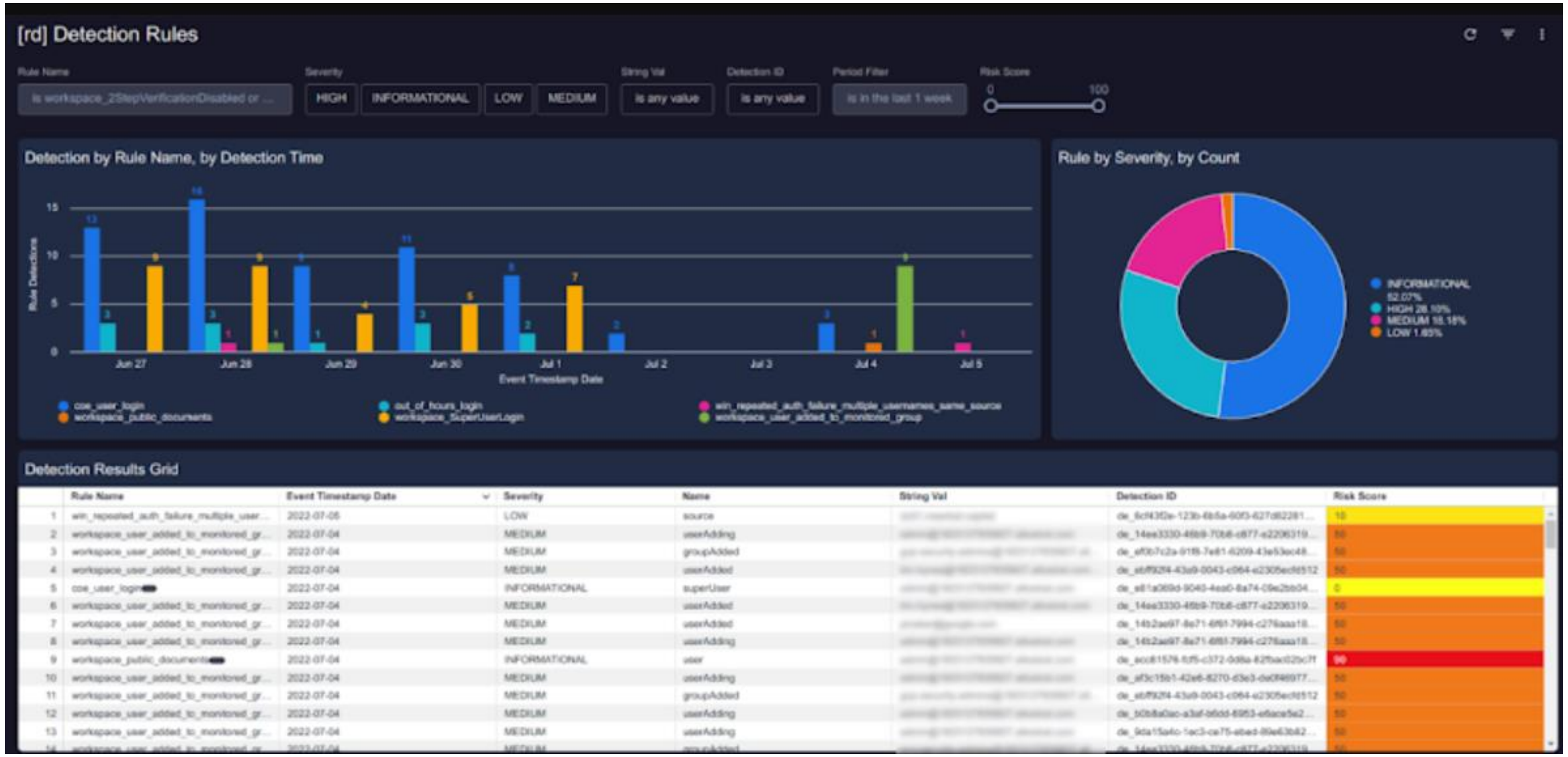
Identification Phase – Operating Systems

INCIDENT RESPONSE

- Unfortunately, some attacks are stealthy, and they are detected later when there is exfiltration.

- In the case of windows and linux systems, incident responder should check:
  - Processes and Services
  - Files
  - Network usage
  - Scheduled tasks
  - Accounts
  - Logs

Identification Phase – Security Monitoring
INCIDENT RESPONSE



Rule Name: is workspace_2StepVerificationDisabled or ...
Severity: HIGH | INFORMATIONAL | LOW | MEDIUM
String Val: is any value
Detection ID: is any value
Period Filter: is in the last 1 week
Risk Score: 0 – 100

Detection Results Grid

	Rule Name	Event Timestamp Date	Severity	Name	String Val	Detection ID	Risk Score
1	win_repeated_auth_failure_multiple_user...	2022-07-05	LOW	source	[redacted]	de_6cf43f2e-123b-6b5a-60f3-627d62281...	10
2	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdding	[redacted]	de_14ea3330-46b9-70b6-c877-e2206319...	50
3	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	groupAdded	[redacted]	de_ef0b7c2a-91f8-7e81-6209-43e53ec48...	50
4	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdded	[redacted]	de_ebff92f4-43a9-0043-c064-e2305ecfd512	50
5	coe_user_login[redacted]	2022-07-04	INFORMATIONAL	superUser	[redacted]	de_e81a069d-9040-4ea0-8a74-09e2bb04...	0
6	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdded	[redacted]	de_14ea3330-46b9-70b6-c877-e2206319...	50
7	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdded	[redacted]	de_14b2ae97-8e71-6f61-7994-c276aaa18...	50
8	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdding	[redacted]	de_14b2ae97-8e71-6f61-7994-c276aaa18...	50
9	workspace_public_documents[redacted]	2022-07-04	INFORMATIONAL	user	[redacted]	de_acc81576-fcf5-c372-0d8a-82fbac02bc7f	90
10	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdding	[redacted]	de_af3c15b1-42e6-8270-d3e3-0a0f46977...	50
11	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	groupAdded	[redacted]	de_ebff92f4-43a9-0043-c064-e2305ecfd512	50
12	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdding	[redacted]	de_b0b8a0ac-a3af-b6dd-6953-e6aca5e2...	50
13	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	userAdding	[redacted]	de_9da15a4c-1ac3-ca75-ebed-89e63b82...	50
14	workspace_user_added_to_monitored_gr...	2022-07-04	MEDIUM	groupAdded	[redacted]	de_14ea3330-46b9-70b6-c877-e2206319...	50

Identification Phase – Is it an Incident?

INCIDENT RESPONSE

To determine if an event is an accident or not:

- **Verifying that it is not a simple error** of some user, admin or others
- **Checking evidence** accurately
- **Wondering if there are any other possibilities**
- Keeping up to date on the general situation and **report everything**.

Identification Phase – Gather Intelligence regarding IoC

INCIDENT RESPONSE

Indicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

URLDNA
BETA
ALIEN VAULT
PhishTank®
VirusTotal
PAYLOAD SECURITY
AbuseIPDB
ANY RUN
MX TOOLBOX®
ThreatCrowd
SHODAN

Containment Phase
INCIDENT RESPONSE

The goal of containment is to **limit damage from the current security incident and prevent any further damage**. Several steps are necessary to completely mitigate the incident, while also preventing destruction of evidence that may be needed for prosecution

- **Questions to address**
- What’s been done to contain the breach short term?
- What’s been done to contain the breach long term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all access credentials been reviewed for legitimacy, hardened and changed?
- Have you applied all recent security patches and updates?

Containment Phase
INCIDENT RESPONSE

- **Short-term containment**—limiting damage before the incident gets worse, usually by isolating network segments, taking down hacked production server and routing to failover.
- **System backup**—taking a forensic image of the affected system(s) with tools such as Forensic Tool Kit (FTK) and only then wipe and reimage the systems. This will preserve evidence from the attack that can be used in court, and also for further investigation of the incident and lessons learned.
- **Long-term containment**—applying temporarily fixes to make it possible to bring production systems back up. The primary focus is removing accounts or backdoors left by attackers on the systems, and addressing the root cause—for example, fixing a broken authentication mechanism or patching a vulnerability that led to the attack.

Containment Phase – Incident Characterization

INCIDENT RESPONSE

- After declaring an incident, we need to record its category (one or more), severity and sensitivity (who should be informed)

- **Category**:
  - DoS, compromised information, compromised assets, illegal activity, hacking, malware, email, policy violation

- **Severity**:
  - Incident impacts critical systems -> response in 60 minutes
  - Incident impacts no-critical systems -> response in 4 hours
  - Possible incident, no-critical -> response within 24 hours

- **Sensitivity**:
  - Extremely sensitive (e.g. CSIRT, mgmt)
  - Sensitive (e.g. CSIRT, mgmt, system administrator, operations)
  - Less sensitive (e.g. alert employee to an isolated virus infection)

Containment Phase – Incident Characterization

INCIDENT RESPONSE

- After declaring an incident, we need to record its category (one or more), severity and sensitivity (who should be informed)
- **Category**:
  - DoS, compromised information, compromised assets, illegal activity, hacking, malware, email, policy violation
- **Severity**:
  - Incident impacts critical systems -> response in 60 minutes
  - Incident impacts no-critical systems -> response in 4 hours
  - Possible incident, no-critical -> response within 24 hours
- **Sensitivity**:
  - Extremely sensitive (e.g. CSIRT, mgmt)
  - Sensitive (e.g. CSIRT, mgmt, system administrator, operations)
  - Less sensitive (e.g. alert employee to an isolated virus infection)

Containment Phase – Order of Volatility

INCIDENT RESPONSE

Gather most volatile evidence first

- CPU, cache and registers
- Routing table, ARP cache, processes
- RAM
- Temp files/swap space
- Hard disk
- Remotely logged data
- Archival media

Containment Phase – Short Term Action
INCIDENT RESPONSE

- Try to prevent the attacker from causing more damage.
- Avoid changing data on disk on compromised machines.
  - This is to obtain "clean" evidence, through a process of creating the disk image
- Some of the short-term actions:
  - **Isolate the switch port using network management tools**, so that the system cannot receive or send data. Alternatively, put it in a Quarantine VLAN
  - **Apply filters to routers and/or firewalls**
  - **Change a name in DNS** to point to a different IP address
  - **If during the short-term containment is necessary disable the system** (e.g. remove it from the network) will be required to notify the business unit responsible for the system
  - **It is necessary to inform the business unit through an email**, so that they can track what happened and get an email in response in which they declare to be aware of the current situation.
  - **The business unit may disagree with your advice to drop the system if it is not of the same opinion**, the business unit (unfortunately) almost always wins!!!!

Containment Phase – Forensic Imaging
INCIDENT RESPONSE

- **Exact copy of a memory,** bit for bit
- Gathers unallocated space and Master File Table
- Time-consuming process
- Examine a copy, not the original
  - You can recover from mistakes
- Server >> Huge Memory

Containment Phase – Forensic Imaging

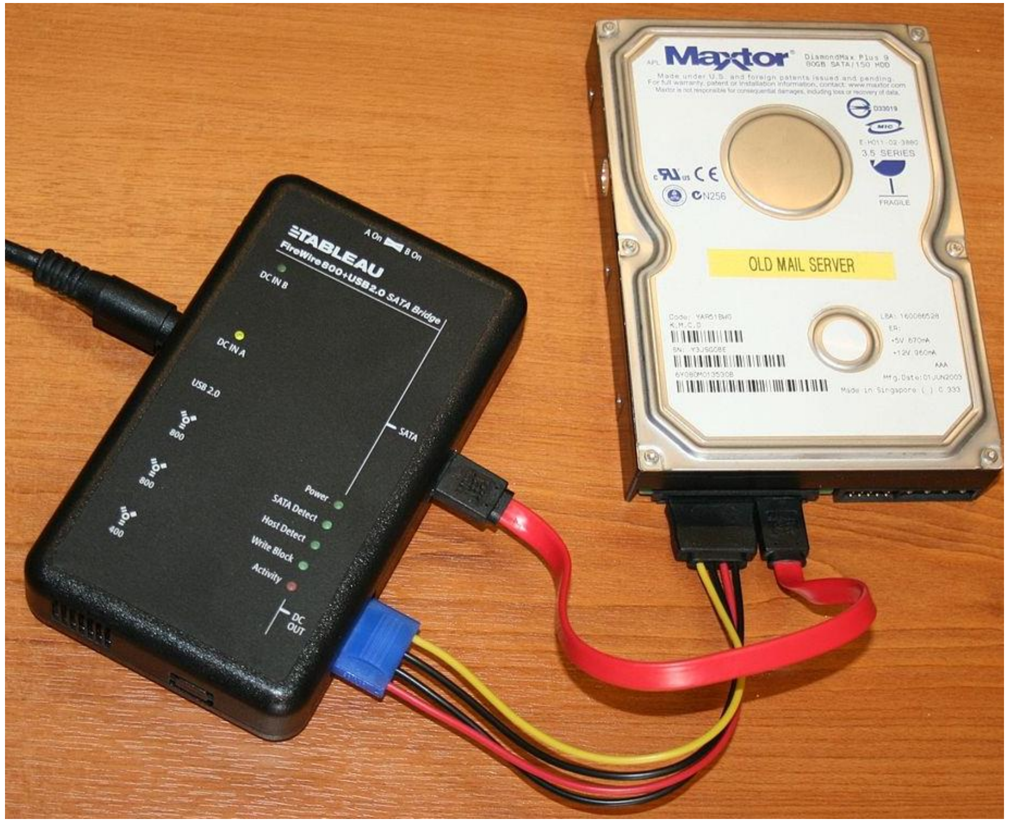
INCIDENT RESPONSE

- Copy one hard drive to another, larger hard drive
- Source drive normally removed from computer
- Critical to use a write-blocker
- Hardware or software
- Forensically clean destination drive first
- Proof of that goes in the case file

- Foresics Image Format:
  - Proprietary
    - EnCase (.E01) – Actually "Expert Witness"
    - AccessData Custom Content Image (.AD1)
  - Open
    - Advanced Forensics Format (AFF)
    - Open format,
    - Raw (.dd or .001)

Containment Phase – Write Blocker

INCIDENT RESPONSE



Containment Phase – Software

INCIDENT RESPONSE

- Software allows you to make a copy of a disk/hard drive and analyze its content.
- FTK Imager creates a 1-to-1 copy of the original disk called a forensic image.
- Autopsy analyzes forensic images to produce reports on the types of files and potential personally identifiable information.

ACCESSDATA®
ForensicToolkit (FTK)

AUTOPSY
DIGITAL FORENSICS

Containment Phase – Volatile Memory Dump

INCIDENT RESPONSE

Memory dumps capture the state of volatile memory at a given instant; can provide information **into network connections, credentials, application data, encryption keys, and other critical data** that are loaded into memory when a process runs

Memory dumps can be **created by dumping a computer’s RAM or by dumping the state and heap of individual processes**

Containment Phase – Volatile Memory Dump

INCIDENT RESPONSE

Memory dumps can be obtained by using memory imaging tools like the following:

- FTK Imager
- procdump
- dd
- FireEye RedLine
- Magnet RAM Capture
- Process Explorer
- jmap

Containment Phase – Software Volatility

INCIDENT RESPONSE

The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples.

The extraction techniques are performed completely independent of the system being investigated but offer visibilty into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.

Containment Phase – Long Term Action
INCIDENT RESPONSE

Once you have obtained the image for forensic analysis, it will be possible to start making changes to the system:

- **Ideal: if the system can be kept offline, move to the eradication step**
- Less ideal, but sometimes necessary: if the system must be kept in production, perform long-term containment actions:
  - Numerous potential actions, including:
  - Patch the system
  - Patch neighboring systems
  - Inserting an IPS
  - Null routing
  - Change passwords
  - Apply routers and/or firewalls filter rules
  - Remove accounts used by attacker
  - Shutdown backdoor processes used by attacker
- **The idea of long-term containment is to apply a temporary fix in production, while preparing a "clean" system during eradication phase.**

Eradication Phase
INCIDENT RESPONSE

Eradication is intended to actually remove malware or other artifacts introduced by the attacks, and fully restore all affected systems.

Questions to address

- Have artifacts/malware from the attacker been securely removed?
- Has the system be hardened, patched, and updates applied?
- Can the system be re-imaged?

Eradication Phase
INCIDENT RESPONSE

Reimaging—complete wipe and re-image of affected system hard drives to ensure any malicious content is removed.

Preventing the root cause—understanding what caused the incident preventing future compromise, for example by patching a vulnerability exploited by the attacker.

Applying basic security best practices—for example, upgrading old software versions and disabling unused services.

Scan for malware—use anti-malware software, or Next-Generation Antivirus (NGAV) if available, to scan affected systems and ensure all malicious content is removed.

Eradication Phase – Improve Defenses

INCIDENT RESPONSE

Some of the actions for improving security can be:

- Implement appropriate protection techniques
- Applying firewalls and/or routers filters
- Moving the system with a new name/IP address
- Generating null routing for a particular IP address
- Changing DNS name
- Applying patches and hardening the system

Recovery Phase
INCIDENT RESPONSE

The goal of recovery is to bring all systems back to full operation, after verifying they are clean and the threat is removed.

Questions to address:

- When can systems be returned to production?
- Have systems been patched, hardened and tested?
- Can the system be restored from a trusted back-up?
- How long will the affected systems be monitored and what will you look for when monitoring?
- What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc)

Recovery Phase
INCIDENT RESPONSE

- **Defining time and date to restore operations**—system owners should make the final decision on when to restore services, based on information from the CSIRT.
- **Test and verifying**—ensuring systems are clean and fully functional as they go live.
- **Monitoring**—ongoing monitoring for some time after the incident to observe operations and check for abnormal behaviors.
- **Do everything to prevent another incident**—considering what can be done on the restored systems to protect them from recurrence of the same incident.

Recovery Phase - Validation

INCIDENT RESPONSE

- Restore the impacted systems back into production in a safe manner
- Validate the system
- Once the system has been restored, verify that the operation was successful, and that the system is back to its normal conditions
- Ask for test plans and documentation
- Retest the system

Recovery Phase - Validation
INCIDENT RESPONSE

- Decide when to restore operations
- Try to restore the system outside of business hour
- This makes it easier to monitor then
- In certain situations, the business unit will want to restore the system immediately, once it is ready
- Leaving the final decision to business unit, trying in any case to give advice on this matter

Recovery Phase – Monitoring

INCIDENT RESPONSE

Monitor the systems once they are back online, continue to:

- Monitor to find any backdoors that have not been detected during the previous phases
- Utilize an IDS and IPS
- If possible, create a custom signature to trigger the original attack vector because the attacker reuses the same attack again
- In addition, check operating system and application logs extra carefully

Recovery Phase – Looking for Artifacts

INCIDENT RESPONSE

One of the most important things that incident managers can do during the recovery phase is to continuously check that there is no further compromise to the system

Attackers will not always use malware; sometimes they will access systems through normal login mechanisms (e.g. SSH, RDP)

It will be necessary to create a script that make a daily checks of systems looking for:

- Look for changes to configuration via registry keys and values
- Look for Unusual processes
- Look for accounts used by the attacker
- Look for simultaneous logins

Lesson Learned Phase

INCIDENT RESPONSE

No later than two weeks from the end of the incident, the CSIRT should compile all relevant information about the incident and extract lessons that can help with future incident response activity.

Questions to address

- What changes need to be made to the security?
- How should employee be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?
- No one wants to go through a data breach, but it's essential to plan for one. Prepare for it, know what to do when it happens, and learn all that you can afterwards.

Lesson Learned Phase

INCIDENT RESPONSE

- **Completing documentation**—it is never possible to document all aspects of an incident while it is going on, and achieving comprehensive documentation is very important to identify lessons for next time.
- **Publishing an incident report—**the report should provide play-by-play review of the entire incident, and answer the Who, What, Where, Why, and How questions.
- **Identify ways to improve CSIRT performance**—extract items from the incident report that were not handled correctly and can be improved for next time.
- **Establish a benchmark for comparison**—derive metrics from the incident report that you can use to guide you in future incidents.
- **Lessons learned meeting**—conduct a meeting with the CSIRT team and other stakeholders to discuss the incident and cement lessons learned that can be implemented immediately.

Lesson Learned Phase - Reporting

INCIDENT RESPONSE

A Security Report should include:

- Executive summary
- Service/system architecture
- Analyzed material
- What happened?
- What are the cause?
- Are there any impacts?
- What are the conclusions and what you have learned?

Lesson Learned Phase – Closing Meeting

INCIDENT RESPONSE

- The meeting should be held as soon as possible
- Possibly within two of resuming production
- Review the report
- Finalize the executive summary
- Based on what has been learned from the incident, the following aspects will be modified and improved:
  - Processes
  - Technologies
  - Improved Incident handling capabilities

References

What would you like clarifications on?

QUESTIONS & ANSWERS

Introduction to Incident Response

Introduction
RANSOMWARE

What is Ransomware?

Ransomware is a kind of malware (*bad computer program*).
It locks up files, computer, server networks and even entire companies.
It asks for money (ransom) to unlock them.

How Does it Work?

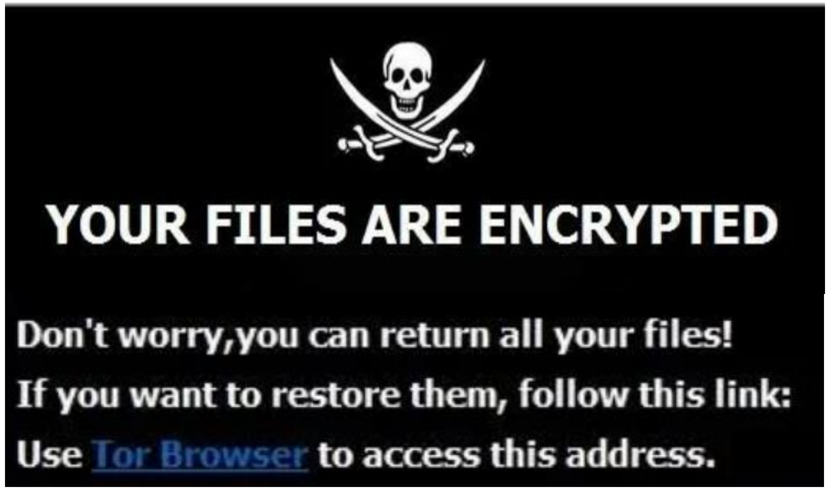
Ransomware uses secret codes to scramble your files so you can't open them (encryption).
The threat actors promise to give the code to unlock if the ransom is paid.

Why Do They Do This?

They work for money, and they use the encrypted files as "hostages" to get it.
Sometimes, they target big companies because they can pay a lot.

How Does Ransomware Get In?

It can come from email attachments, sketchy websites, or weak spots in network's defences.
Clicking on the wrong thing can let it in.

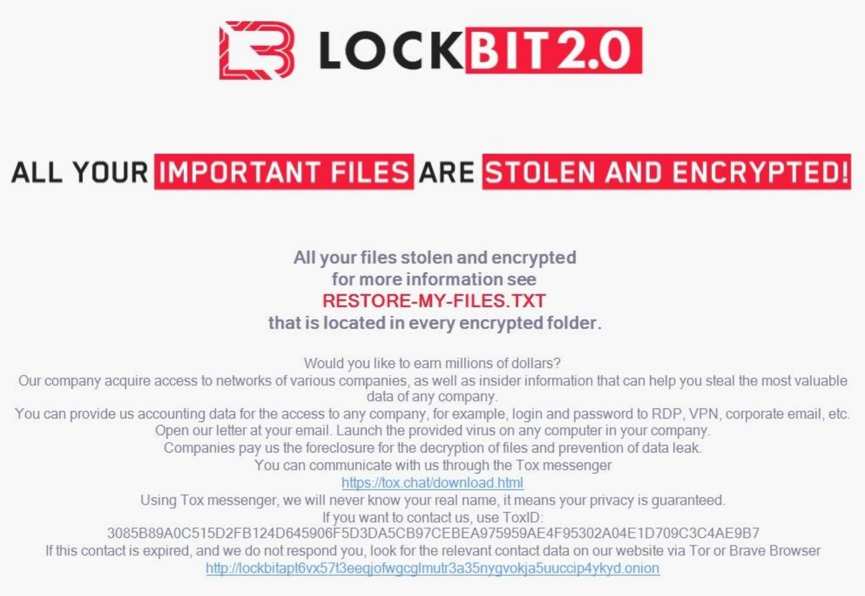


YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, follow this link:
Use Tor Browser to access this address.

Introduction
RANSOMWARE

- Cyber-criminals have adapted their techniques, rather than just encrypting files, double extortion ransomware exfiltrates the data first and than encrypt.
- If the victim does not pay, the attackers will publish data (strategic plans, GDPR relevant data, C-LEVEL email…).
- Ransomware triple extortion involves cybercriminals threatening victims of data theft (e.g., customer of the company) and public exposure if a ransom is not paid.


LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

Ransomware
EVOLUTION

- In the past five years, ransomware attacks have evolved from rare incidents into common and disruptive threats.
- Ransomware demands and payments hit record highs in 2021 ($939.9 million).
- Despite sanctions, ransomware payments are on record-breaking trajectory for 2023 (> $1 billion).
- Ransomware have evolved into the most lucrative form of cybercrime.
- Cyber Gangs are organized in companies, financially motivated, not isolated cyber criminal.
- Not automated-only attack, there are people which perpetrate the attacks.

Ransomware

RANSOMWARE AS A SERVICE

"RaaS (Ransomware as a Service) is a criminal business model provided as a service, where the breach is carried out by a group of highly organized cybercriminals."

Level 1

Developer

Programming experts who engage in writing malware and develop command and control dashboards for affiliates

Level 2

Affiliate

They rent the ransomware from developers to **carry out the actual attack** and extortion activities.

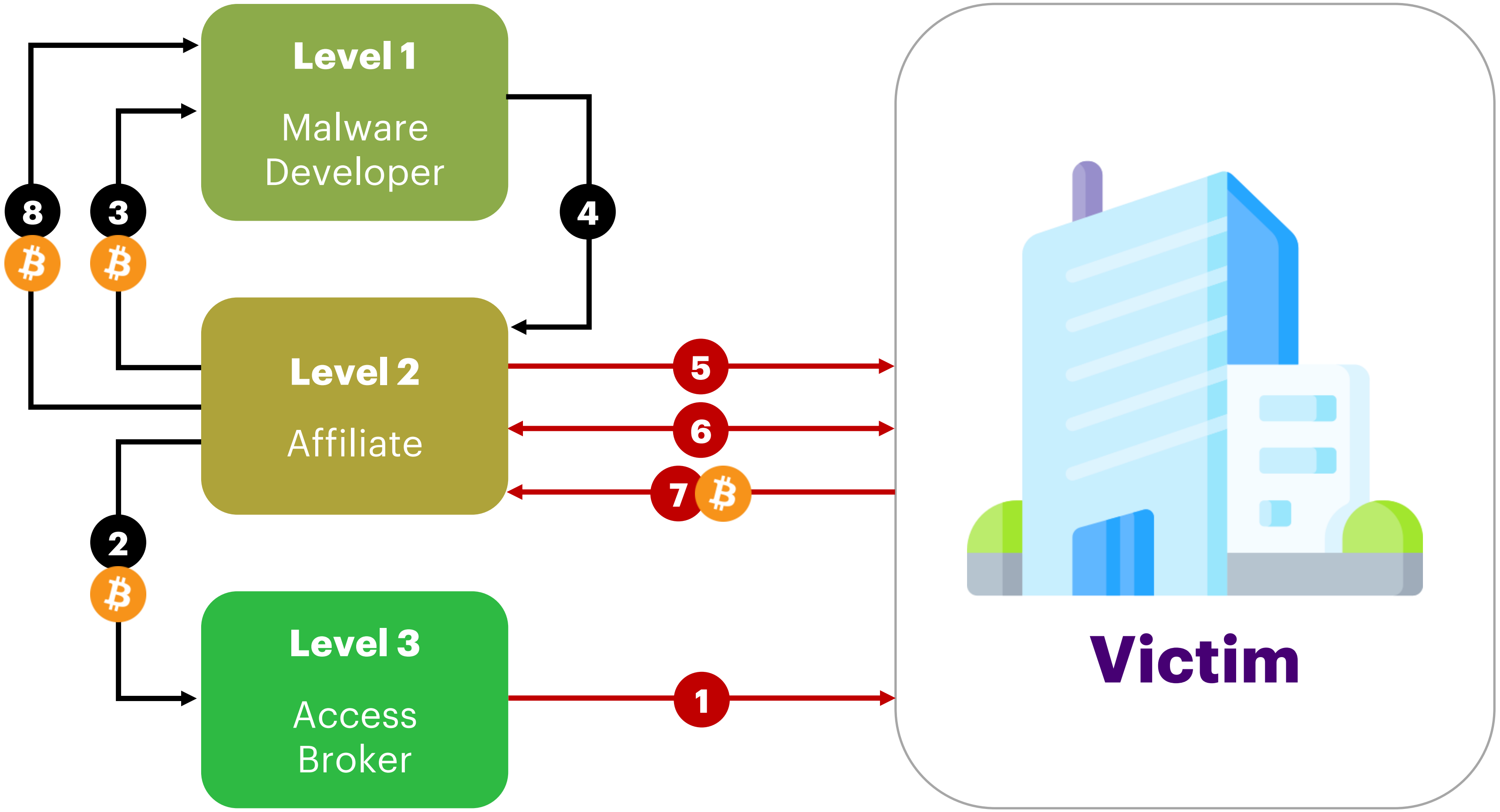
Level 3

Access Broker

Cybercriminals who breach companies to gain access to their networks and sell them on Dark Web forums.

Ransomware

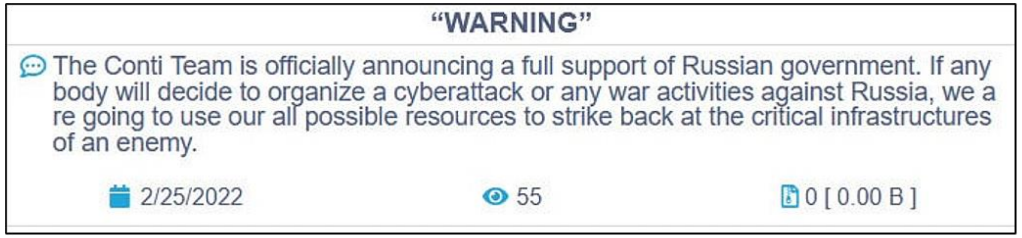
RANSOMWARE AS A SERVICE



Ransomware

CONTI – INSIGHT FROM INTERNAL CHAT

- Conti is ransomware gang that was active between 2020 – 2022.
- The software, for encrypt file, uses its own implementation of AES-256 that uses up to 32 individual logical threads, making it much faster than most ransomware
- Huge attack infrastructure, a lot of handbook and tutorial to launch attacks.
- Conti ransomware operations made $200 millions (*estimated value by Chainalysis*)
- Very early on in the Russian-Ukrainian Crisis, Conti made a public statement where they expressed their loyalty to the Russian Administration.
- As a reaction to this statement and the current conflict, a Ukrainian security researcher, operating by the twitter handle @contileaks decided to publish years of Conti's internal Jabber conversations online.



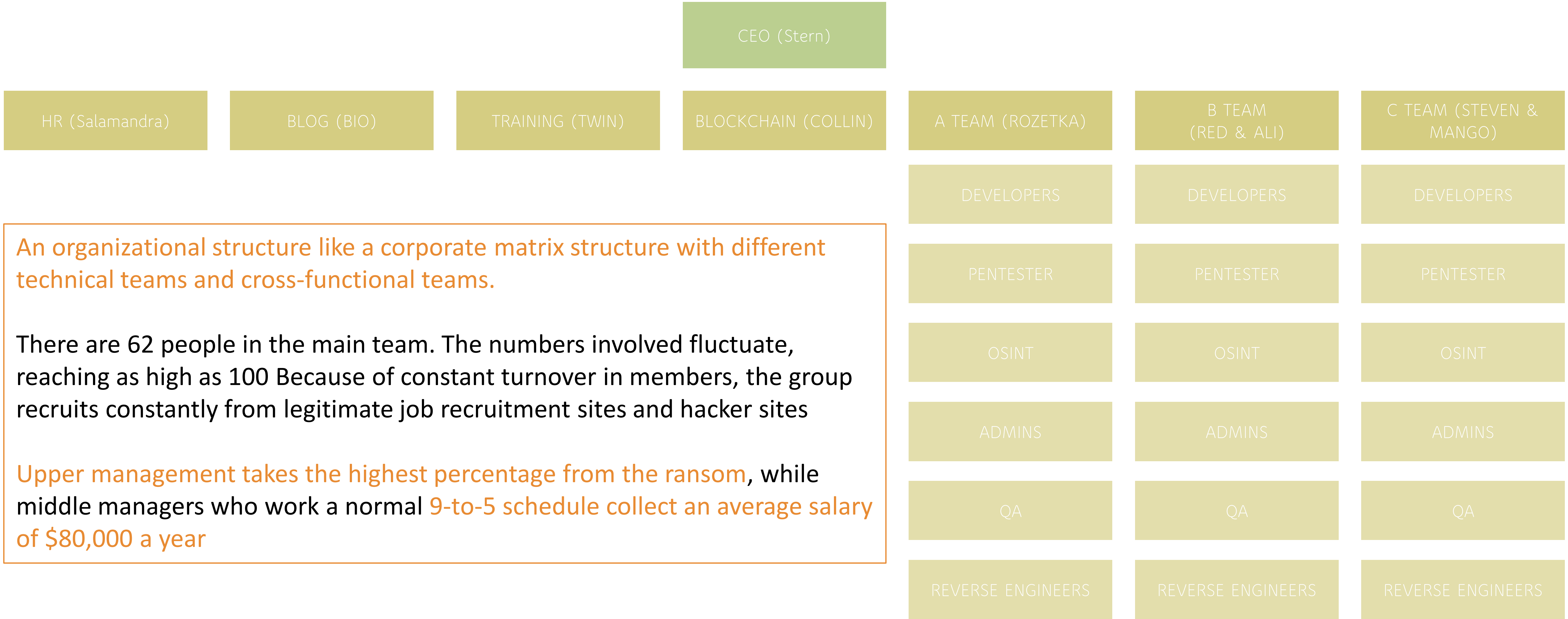
"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we a re going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 55 0 [0.00 B]

Ransomware

CONTI – ORG CHART



CEO (Stern)

HR (Salamandra)

BLOG (BIO)

TRAINING (TWIN)

BLOCKCHAIN (COLLIN)

A TEAM (ROZETKA)	B TEAM (RED & ALI)	C TEAM (STEVEN & MANGO)
DEVELOPERS	DEVELOPERS	DEVELOPERS
PENTESTER	PENTESTER	PENTESTER
OSINT	OSINT	OSINT
ADMINS	ADMINS	ADMINS
QA	QA	QA
REVERSE ENGINEERS	REVERSE ENGINEERS	REVERSE ENGINEERS

An organizational structure like a corporate matrix structure with different technical teams and cross-functional teams.

There are 62 people in the main team. The numbers involved fluctuate, reaching as high as 100 Because of constant turnover in members, the group recruits constantly from legitimate job recruitment sites and hacker sites

Upper management takes the highest percentage from the ransom, while middle managers who work a normal 9-to-5 schedule collect an average salary of $80,000 a year

Ransomware

COST OF AN INCIDENT

The global average cost of a data breach in 2023 reached a record high of $4.45 million.
This cost increased by 2.3% compared to the previous year and by 15.3% compared to 2020.

Factors Affecting Data Breach Costs:

Several factors influence data breach costs, including incident type, severity, regulatory standards, company size, sector, and region.

Not only an IT cost

Regulation and Litigation Costs:

- Strict data protection laws and litigation result in substantial fines, settlements, and legal fees.
- Highly regulated industries, like healthcare and finance, often face higher costs due to non-compliance fines.

Business Downtime Costs:

- Business downtime can be costly, particularly for technology-dependent firms.
- Manufacturing companies can lose millions of dollars per day during downtime.

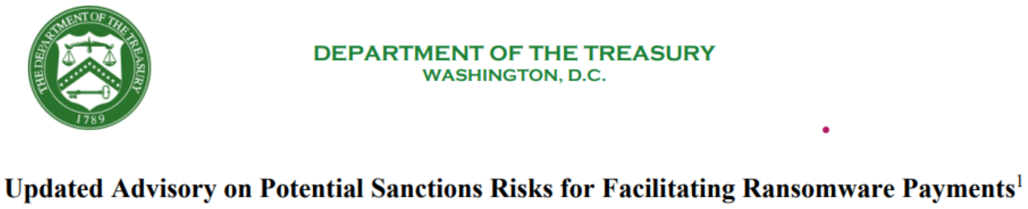
Reputation Damage and Customer Trust:

- Reputational damage remains a significant cost of data breaches, impacting customer trust.
- Loss of intellectual property can also be a major cost factor.

Ransomware

RISK OF PAYING A RANSOMWARE

- Before the Russia invasion of Ukraine, 75% of ransomware payments went to Russia.
- Paying ransoms to Russian entities is now a political issue due to Russia's war against Ukraine.
- Paying ransoms to Russia, a sanctioned country, has legal consequences.
- Russian sanctions are broad, and it is not easy to understand them.
- Sanctions aim to combat ransomware by disrupting gangs, making cryptocurrency laundering harder, and addressing safe harbors.
- Violating sanctions by paying ransoms can result in fines up to $1 million and 20 years in prison per violation.
- OFAC's list of sanctioned groups is specific, while country-wide sanctions like those on Russia are broader.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

DON'T PAY THE RANSOM

Ransomware
CONSIDERATION

62%

of companies that paid ransomware were able to restore data

13%

Of companies were able to restore data from backup

5%

Of companies were not able to restore from backup and did not pay.

20%

of companies that paid ransomware were not able to restore data

Uncertainty of Ransom Payments:

- Paying a ransom does not guarantee data or system access recovery.
- There are instances of payments resulting in no decryption or faulty decryption tools.
- Victims may be targeted again by different attackers using the same vulnerability.

DON’T PAY THE RANSOM

**data from a https://www.veeam.com/it/analyst-reports/ransomware-trends-executive-summary-europe_wpp.pdf*

Ransomware

COST OF AN INCIDENT

Name and release year of the attack	Loss
WannaCry (2017)	*4 billion USD*
NotPetya (2017)	*10 billion USD*
Sodinokibi (2019)	*200 million*
Ransomware attack on Colonial Pipeline (2021)	*4.4 million USD*
Ransomware attack on Impressa (2022)	*50 terabytes of data*
Ransomware attack on Costa Rica Government (2022)	*30 million USD / day*
Ransomware attack on Swisspost (2022)	*1.6 terabytes data*

https://www.statista.com/statistics/1410605/largest-ransomware-attacks-worldwide/

**data from a https://www.veeam.com/it/analyst-reports/ransomware-trends-executive-summary-europe_wpp.pdf*

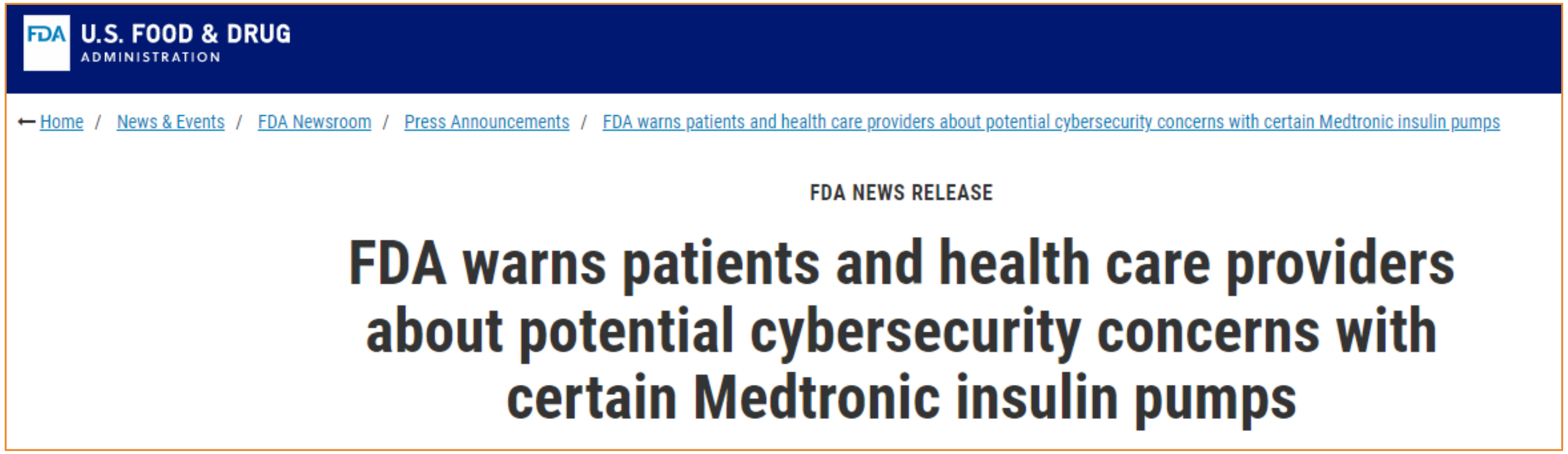
Ransomware

REAL CASE

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system. suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.
- The Colonial Pipeline Company halted all pipeline operations to contain the attack.
- About 45% of all fuel consumed on the U.S. East Coast arrives via the pipeline system.
- U.S. President Joe Biden declared a state of emergency for 17 states.
- Company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million)
- It was the largest cyberattack on an oil infrastructure target in the history of the United States. The attack was conducted by DarkSide Gang.

Conclusion

WHAT'S NEXT?

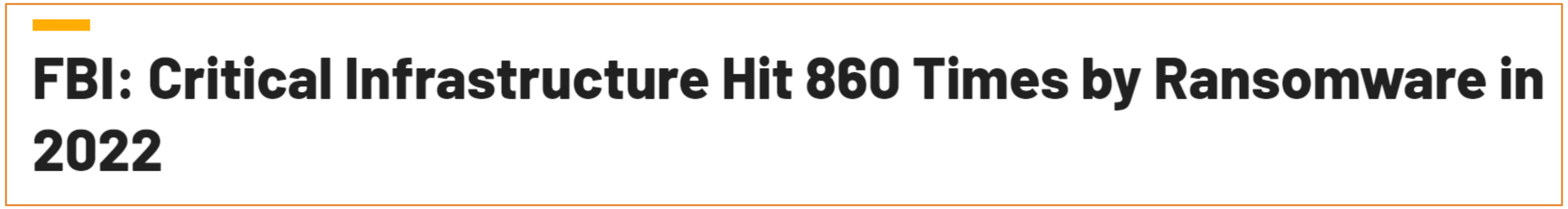


U.S. FOOD & DRUG ADMINISTRATION

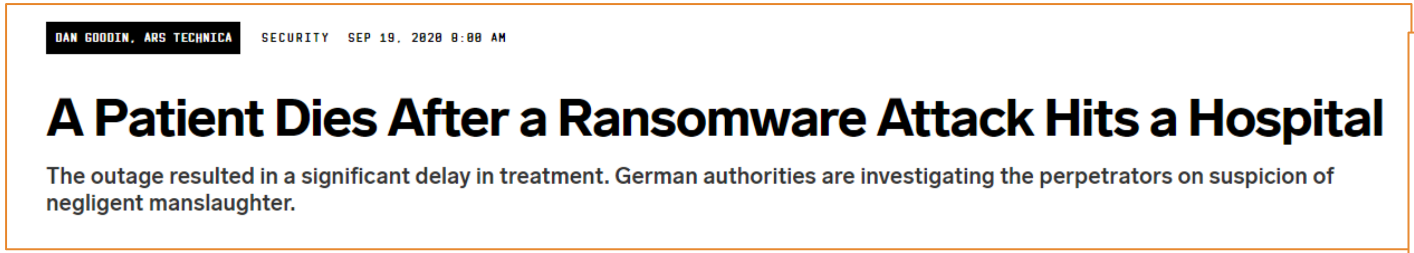
← Home / News & Events / FDA Newsroom / Press Announcements / FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps

FDA NEWS RELEASE

FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps



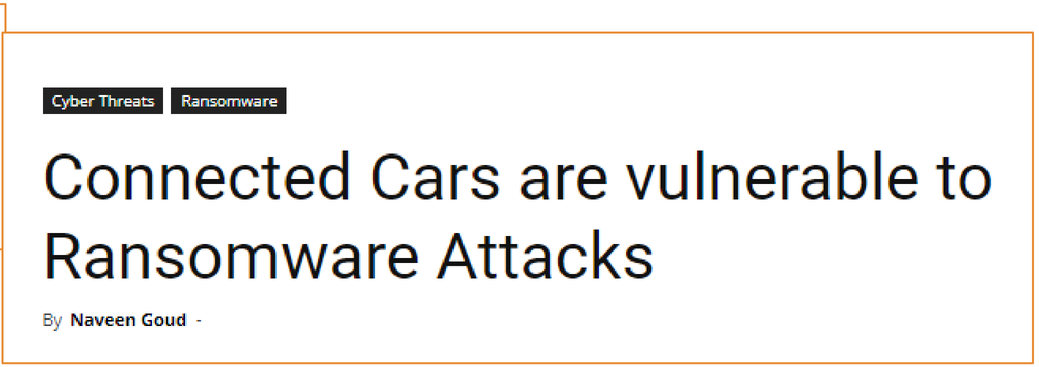
FBI: Critical Infrastructure Hit 860 Times by Ransomware in 2022



DAN GOODIN, ARS TECHNICA SECURITY SEP 19, 2020 8:00 AM

A Patient Dies After a Ransomware Attack Hits a Hospital

The outage resulted in a significant delay in treatment. German authorities are investigating the perpetrators on suspicion of negligent manslaughter.



Cyber Threats Ransomware

Connected Cars are vulnerable to Ransomware Attacks

By **Naveen Goud** -

Let’s connect!

Linkedin: https://www.linkedin.com/in/redaelli/

X: twitter.com/solventred

References

- https://www.varonis.com/blog
- https://www.cynet.com/incident-response/
- https://www.statista.com/statistics/1410605/largest-ransomware-attacks-worldwide/
- *https://www.veeam.com/it/analyst-reports/ransomware-trends-executive-summary-europe_wpp.pdf*